

Protection in Elastic Optical Networks Against up to Two Failures Based FIPP p -Cycle

Helder M. N. S. Oliveira and Nelson L. S. da Fonseca
 Institute of Computing - University of Campinas
 Campinas 13089-971, SP, Brazil
 Email: helder@lrc.ic.unicamp.br, nfonseca@ic.unicamp.br

Abstract—Optical networks are subject to faults in links and nodes which can cause massive data loss. In the literature, many techniques have been proposed to deal with such failures in order to support continuous network operation. One of these techniques defines p -Cycles which provide ring-type protection and the speed of restoration of meshes. Moreover, Flexgrid networks emerged as a solution to deal with the diverse requirements of bandwidth. This paper presents two new algorithms to provide path protection using p -cycle path networks in Flexgrid networks. Our algorithms provide 100 % protection against single failure as well as against two failures.

Keywords—Elastic Optical Networks, Protection, p -Cycle

I. INTRODUÇÃO

Uma das principais características da arquitetura da Internet é não impor restrição sobre a camada de aplicação, permitindo, assim, o surgimento de novas aplicações. Essas aplicações têm demandas heterogêneas de largura de banda. Enquanto algumas aplicações, tais como e-mails requisitam pouca demanda de largura de banda, outras como IPTV e aplicações de *grid* requisitam largura de banda na ordem de Gbits por segundo [1]. Tal diversidade exige uma rede de transporte flexível no que tange ao provisionamento de banda passante.

A técnica de multiplexação por divisão de comprimento de onda (WDM) empregada na camada de enlace da Internet possibilita a disponibilidade de grande capacidade e permite a multiplexação de vários comprimentos de onda em uma única fibra. WDM aloca faixas de frequência de largura fixa, o que leva a um conjunto de comprimentos de onda com a mesma capacidade separados por uma frequência de banda de guarda. Tal alocação leva à subutilização do espectro uma vez que as demandas raramente coincidem com a capacidade de um comprimento de onda. Em WDM, a capacidade de um comprimento de onda pode acomodar demandas de diferentes tamanhos através do emprego de agregação de tráfego (*traffic grooming*), porém esta técnica implica em *overhead* e não elimina por completo o problema do desperdício de capacidade. Apesar da tecnologia de WDM com múltiplas taxas apresentar alguma flexibilidade na alocação de recursos, sua granularidade de alocação é “grossa” e só melhora limitadamente o problema de desperdício de capacidade.

Tal rigidez de alocação de espectro motivou o surgimento de redes elásticas cujo espectro pode ser alocado com granularidade “fina” (spectrum-sliced elastic optical network), o que possibilita a alocação de faixas do espectro de tamanho variável. Redes ópticas elásticas empregam a multiplexação por divisão de frequências ortogonais (OFDM). OFDM é uma

tecnologia de transmissão multi-portadora, que divide canais subportadoras ortogonais de menor capacidade.

Por ser um meio cabeado, as fibras ópticas são propensas a cortes. Dada a enorme capacidade de uma fibra óptica, qualquer interrupção implica em grandes perda de dados. Tal vulnerabilidade tem motivado o desenvolvimento de diferentes esquemas de restauração e proteção. p -Cycle é uma dessas técnicas de proteção, cujo emprego foi investigado intensamente em redes WDM. p -Cycles combinam as propriedades de proteção da topologia em anel de recuperação rápida e a eficiência de proteção das redes de malha restauráveis. p -Cycles protegem os enlaces que cobrem, bem como os enlaces que tem seus pontos finais no p -cycle (“enlaces tranzonais”). Um tipo de p -cycle de interesse especial é o p -cycle FIPP (*Failure-Independent Path Protecting*) que fornece caminhos de proteção pre-conectados.

No entanto, a grande dificuldade no projeto de redes que empregam p -cycles para proteção é a complexidade computacional para obter a solução do problema de provisão de proteção, que é exponencialmente dependente do número de nós e do número de enlaces. O problema de estabelecimento de caminhos protegidos por p -cycles é um problema NP-completo e heurísticas têm sido desenvolvidas para resolvê-lo. O presente artigo introduz dois algoritmos chamados FIPP-Flex e FIPP-Flex-twofailure para proteção de caminhos através do uso de p -cycle FIPP em redes ópticas elásticas (*Flexgrid*). O algoritmo FIPP-Flex provê proteção contra uma única falha e o algoritmo FIPP-Flex-twofailure provê proteção contra ocorrência de duas falhas simultâneas. Os algoritmos promovem compartilhamento de caminhos de proteção com o maior número de caminhos primários possível.

Este artigo está organizado da seguinte forma. A seção II revisa trabalhos relacionados. A seção III introduz os conceitos de p -cycle e FIPP. A seção IV apresenta a notação usada no artigo. A seção V introduz os algoritmos RSA-FLEX e a seção VI apresenta os algoritmos FIPP-FLEX e o FIPP-Flex-twofailure. A seção VII avalia o desempenho do algoritmo proposto e a seção VIII conclui o artigo.

II. TRABALHOS RELACIONADOS

Apesar de terem sido propostos diversos algoritmos de roteamento e alocação de espectro (routing and spectrum allocation - RSA), pouca atenção tem sido dada a questão de proteção em redes elásticas.

Foi proposto em [2] um mecanismo que atua nos transponders ociosos no nó de origem de uma requisição de enlace

de alta taxa de dados para fragmentá-lo em vários de baixa taxa de dados, mais facilmente alocável na rede. Além disso, com o objetivo de apoiar a operação, um algoritmo RSA foi também proposto para alocar adequadamente os fragmentos gerados ao longo do espectro. Para fragmentar a demanda de banda passante da requisição em várias demandas com menor requisição de banda mais facilmente alocáveis na rede.

Em [3] os requisitos de nós ópticos em redes ópticas elásticas foram estudados e múltiplas arquiteturas de rede usando um esquema de alocação de recurso integrado foram comparadas.

Os autores de [4] propuseram políticas conservadoras de proteção em redes ópticas baseadas em OFDM com alocação de banda elástica. Eles introduziram uma política em que caminhos ópticos de *backup* protegem caminhos ópticos primários utilizando caminhos disjuntos, o que leva a maior robustez a proteção.

Os autores em [5] propuseram técnica de sobrevivência “transparente” em redes ópticas WDM (fwdm). Os autores utilizam a política *First-Fit* para atribuir espectro para os “caminhos de trabalho” e a política *Last-Fit* para atribuir espectro para os “caminhos de *backup*”. O espectro de *backup* de diferentes caminhos podem se sobrepor. A abordagem de proteção proposta, chamada *elastic separate-protection-at-connection* (ESPAC), fornece proteção fim a fim.

Em Liu *et al.* [6], os autores propuseram uma nova técnica para a proteção compartilhada que proporciona aos caminhos ópticos primários compartilhar o espectro de caminhos de *backup* se os caminhos primários forem disjuntos fisicamente.

Nenhum dos trabalhos mencionados anteriormente emprega *p-cycle* para proteção de caminhos.

III. P-CYCLE

O *p-cycle* é um esquema de proteção em que a capacidade reservada é pre-conectada e forma estruturas em anel para proteção de redes em malha [7]. *p-Cycles* fornecem proteção semelhante a proteção fornecida por Anéis de Comutação de Linhas Bidirecionais (BLSR), que é considerado uma generalização do esquema de proteção 1:1 [8]. A diferença fundamental entre *p-cycle* e proteção em anel é a proteção de enlaces transzonais, que são enlaces que não estão no anel (ciclo) porém os dois nós finais estão. Esta propriedade melhora a eficiência de proteção dos *p-cycles*. Outra propriedade importante é a ausência da necessidade de caminhos comporem rotas em anel, a fim de serem protegidos. *p-Cycles* proveem rápida restauração pois são pre-conectados [9].

A Figura 1 ilustra o conceito de *p-cycle*. Na figura, uma linha simples representa um enlace, um ciclo em negrito representa o *p-cycle* e a seta representa o caminho de recuperação de uma falha denotada por um “X”. Na figura 1(a), A-B-C-D-E-A é um *p-cycle* que usa a capacidade reservada nos enlaces de proteção. Quando o enlace A-B falha, a proteção é provisionada como ilustrado na figura 1(b). Quando o enlace transzonal B-D falha, cada *p-cycle* proporciona dois caminhos alternativos como mostram as figuras 1 (c) e 1(d).

Um caso especial de *p-cycle* para proteção de caminho é o chamado *p-cycle* de Proteção de Caminho com Independência

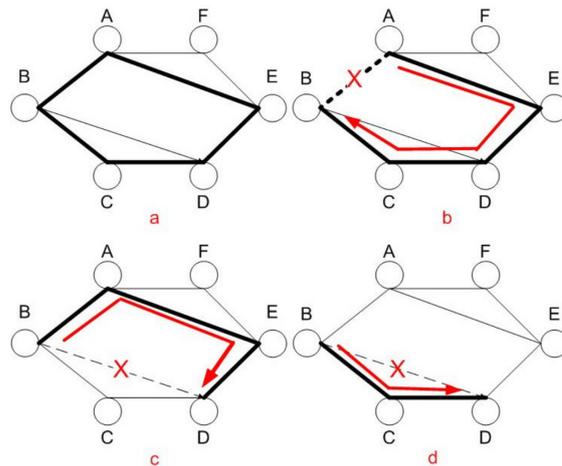


Figure 1: Exemplo de *p-cycle*

de Falha (FIPP) [10]. *p-Cycles* FIPP fornecem proteção de caminhos para caminhos com nós finais sobre o *p-cycle*.

FIPP é uma extensão do conceito de *p-cycle* que permite que falhas não sejam necessariamente limitadas a um enlace ou segmento de caminho imediatamente adjacente aos nós terminais. FIPPs baseiam-se em diferentes “caminhos de trabalho” e de “*backup*”, e proporciona a vantagem de que a detecção de falha é independente da localização da falha, ou seja, é “independente de falha”. Tal propriedade é vantajosa quando a localização da falha é lenta ou difícil, como em redes transparentes e translúcidas [10].

A Proteção por compartilhamento de caminhos de reserva (SBPP) propostas para redes baseadas em sinalização IP também tem a propriedade de falhas independentes. No entanto, a principal diferença entre SBPP e FIPP é que em SBPP o caminho de *backup* precisa ser determinado em tempo real, em caso de falha, o que pode levar a adoção de um caminho de restauração sem a qualidade de transmissão adequada. Por outro lado em FIPP, caminhos de proteção pre-conectado são muito importantes para assegurar a QOS desejada. Além disso, SBPP exige uma extensa base de dados, devido à necessidade de todos os nós terem conhecimento da capacidade global, topologia e compartilhamento de caminho de *backup*.

A Figura 2 ilustra o conceito de *p-cycle* FIPP. Na Figura 2, o ciclo em destaque EFGHIQRONM representa o *p-cycle* e as setas mostram os vários caminhos que são protegidos. Nesses caminhos, estão tanto enlaces transzonais quanto enlaces do próprio *p-cycle*. Pode-se observar que um único *p-cycle* protege um conjunto de catorze caminhos mutuamente excludentes e que possuem seus nós de extremidade no *p-cycle* de caminho.

IV. NOTAÇÃO

A fim de facilitar a compreensão dos algoritmos propostos, a presente seção introduz a notação usada no artigo. Seja:

s: o nó fonte;

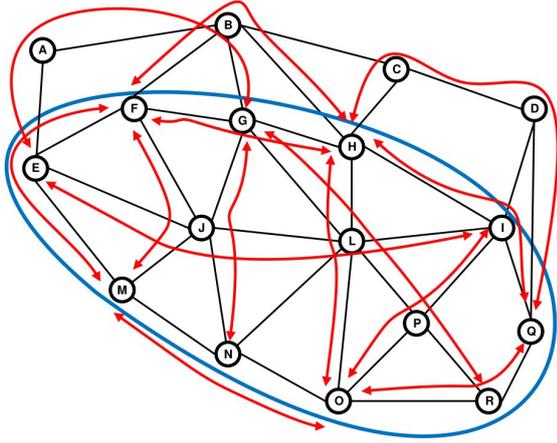


Figure 2: Exemplo de p-cycle FIPP

d : o nó destino;

b : a demanda de largura de banda nos *slots*, $b = 1 \dots B$;

$r(s, d, b)$: requisição do nó s para o nó d com demanda de largura de banda b em *slots*;

N : número de *slots* entre dois nós;

$G = (V, E, W)$: multigrafo marcado composto por um conjunto de nós V , um conjunto de arestas E e um conjunto de pesos das arestas W , $|E| = N \cdot |V|$.

$E = \{e_{u,v,n}\}$: conjunto de n arestas;

$e_{u,v,n}$: a n -ésima arestas conectando os nós u e v ;

$w(e_{u,v,n})$: o peso das arestas $e_{u,v,n}$;

$c(e_{u,v,n}) = 1$ se o n -ésimo *slot* no enlace conectando os nós u e v estão livres e $w(e_{u,v,n}) = \infty$ se o *slot* está alocado;

$W = \{c(e_{u,v,n})\}$: conjunto de pesos das arestas;

$\tilde{G}_{n,b} = (\tilde{V}, \tilde{E}, \tilde{C})$: O n -ésimo grafo marcado tal que \tilde{E} é o conjunto de arestas conectando $\{\tilde{u}, \tilde{v}\} \in \tilde{V}$ e \tilde{C} é o conjunto de custos associados a \tilde{E} . As arestas em \tilde{E} correspondem ao mapeamento de b arestas de G , sendo a primeira aresta a n -ésima aresta conectando u e v .

$\tilde{V} = V$: conjunto de nós;

$\tilde{e}_{u,v} \in \tilde{E}$: arestas conectando \tilde{u} e \tilde{v} ; $\tilde{e}_{\tilde{u},\tilde{v}} = \{e_{u,v,n}\} \in E$ é uma sequência tal que $e_{u,v,n}$ é a menor aresta ordenada, $e_{u,v,n+b}$ é a maior aresta ordenada e $|\tilde{e}_{u,v}| = b$;

$\tilde{w}_n(\tilde{e}_{\tilde{u},\tilde{v}})$: peso da aresta $\tilde{e}_{\tilde{u},\tilde{v}}$;

$\tilde{W}_n = \{\tilde{c}_n(\tilde{e}_{\tilde{u},\tilde{v}})\}$: conjunto de pesos de arestas;

P_n : sequência de arestas \tilde{G}_n tal que o nó fonte s é o menor nó ordenado e d é o maior nó ordenado;

$W(\tilde{P}_n)$: $\sum_{\tilde{e}_{\tilde{u},\tilde{v}} \in \{\tilde{P}_n\}} \tilde{e}_{\tilde{u},\tilde{v}}$: o peso do caminho \tilde{P}_n é a soma dos pesos de todos as arestas na cadeia;

$W_{s,d}$ = peso do menor caminho entre s e d ;

$\tilde{c}_{u,v,b}$: p -cycle que contém os vértices u e v e arestas correspondentes ao mapeamento de b arestas do multigrafo G ;

$\tilde{C}_{u,v,b} = \tilde{c}_{u,v,b}$: conjunto de todos os p -cycles que contém os vértices u e v e arestas correspondentes ao mapeamento de b arestas do multigrafo G ;

\tilde{C} : conjunto de todos os p -cycles estabelecidos;

$P_1 \oplus P_2$: concatenação de dois caminhos P_1 e P_2

V. O ALGORITMO RSA-FLEX

Solução do problema de roteamento e atribuição de comprimentos de onda (RWA) em redes WDM são semelhantes as soluções do problema de roteamento e alocação de espectro (RSA) em redes ópticas *Flexgrid*. Além da restrição de continuidade de espectro que impõe a utilização do mesmo espectro em cada fibra ao longo da rota de um caminho óptico, nos algoritmos RSA *slots* devem ser alocados de forma contínua no espectro (restrição de contiguidade do espectro).

O problema de roteamento e alocação de espectro é um problema NP-difícil [11] e heurísticas são necessárias para resolver o problema. Os algoritmos propostos neste artigo modelam a disponibilidade de espectro na rede como um multigrafo rotulado. Um multigrafo é um grafo que pode ter várias arestas (também chamadas de "arestas paralelas"), conectando o mesmo par de nós. Neste grafo, os vértices representam OXCs e as arestas representam os *slots* dos enlace que conectam os OXCs. Nos multigrafos utilizados no presente artigo, todos os vértices são conectados por N arestas, que é o número de *slots* no espectro de cada enlace da rede. O $W_{s,d}$ representa a disponibilidade de *slots*. O valor ∞ significa que o *slot* já está alocado enquanto o valor 1 significa que o *slot* está disponível para alocação. Estes valores foram definidos para facilitar o emprego de algoritmos tradicionais que encontram o caminho mais curto.

No procedimento proposto, o multigrafo é transformado em $N - b + 1$ grafos, sendo b a demanda de largura de banda em *slots* requisitada. Estes grafos são gerados através da seleção de uma aresta no multigrafo e das b arestas consecutivas a aresta selecionada. Este conjunto de b arestas do multigrafo é mapeada em uma única aresta do grafo gerado. Seu peso é dado pela aplicação de uma função de peso específica, que considera o peso das b arestas. A Figura 3 ilustra um multigrafo representando o espectro e um dos grafos gerado. Para cada grafo gerado, executa-se um algoritmo de caminho mais curto e o caminho escolhido é o que tem o menor peso entre todos os caminhos mais curtos encontrados.

Para uma demanda de b *slots*, $N - b + 1$ grafos do tipo $\tilde{G}_{n,b}$ são gerados. Cada aresta do grafo $\tilde{G}_{n,b}$ corresponde ao mapeamento de b arestas de G iniciando na n -ésima aresta de G . Uma vez que as mesmas arestas ordenadas conectando dois nós em G são mapeadas em arestas de $\tilde{G}_{n,b}$, a continuidade do espectro é garantida.

O algoritmo 1 detalha o algoritmo RSA-Flex. Neste algoritmo, a linha 1 estabelece o conjunto de arestas que será mapeada para $\tilde{G}_{n,b}$ arestas. A linha 2 resolve um algoritmo de menor caminho para o grafo $\tilde{G}_{n,b}$ e provê o menor caminho e seu respectivo peso. Se o peso do caminho mais curto for

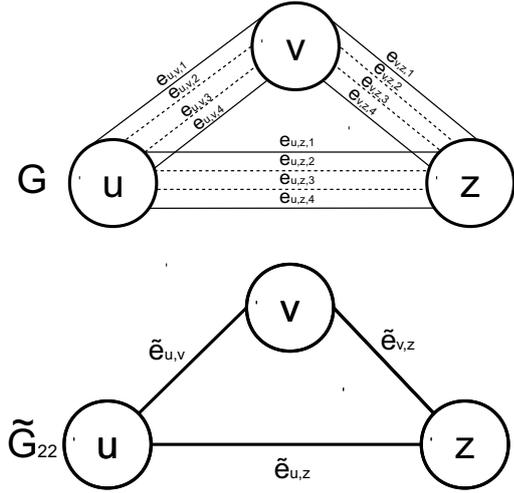


Figure 3: Multigrafo em um grafo associado

Algorithm 1 RSA-Flex

```

1:  $\forall n = 1 \dots N - b$ 
2:  $(W(P_n), P_n) = \text{ShortestPath}(\tilde{G}_{n,b}, r(s, d, b))$ 
3:  $W_{s,d} = W(P_n) \mid \forall i W(P_n) \leq W(P_i)$ 
4: if  $W_{s,d} = \infty$  then
5:    $\text{block } r(s, d, b)$ 
6: else
7:    $W(e_{u,v,i}) = \infty \quad \forall \{u, v\} \in \tilde{P}_i \quad n = n \dots i + b - 1$ 
8: end if

```

∞ , não é possível encontrar um caminho com a restrição de continuidade para a demanda b com alocação começando com o n -ésimo *slot*. A linha 3 seleciona o caminho entre os $N - b + 1$ caminhos mais curtos, com o menor peso. No caso do peso de todos o caminhos mais curto serem ∞ (linha 4), não existe caminho na rede que satisfaça a requisição de b *slots*, portanto, a requisição tem de ser bloqueada (Linha 5). Caso contrário, o caminho mais curto com o menor peso será escolhido (linha 7) e as arestas correspondentes no multigrafo G terão seu peso alterado para ∞ (linha 8), o que significa que os *slots* são alocados para o caminho óptico recém-estabelecido.

Uma vez que o algoritmo RSA-Flex executa um algoritmo de caminho mais curto $N - b$ vezes e considerando o uso do algoritmo de caminho mais curto de Dijkstra, a complexidade computacional do algoritmo proposto é $N \cdot (|V| + |E|) \cdot \log(|V|)$.

VI. ALGORITMOS FIPP-FLEX E FIPP-FLEX-TWOFailure

Os algoritmos apresentados nesta seção, chamados FIPP-Flex e FIPP-Flex-twofailure, resolvem o estabelecimento de caminhos ópticos em redes protegidas por p -cycles FIPP. Nesses algoritmos, caminhos ópticos são estabelecidos se e somente se puderem ser protegidos por um p -cycle FIPP, que protegem somente caminhos primários disjuntos. Requisições

Algorithm 2 FIPP-Flex

```

1:  $(W(P_n), P_n) = \text{RSA-Flex}(G, s, d, b)$ 
2: if  $W_{s,d} = \infty$  then
3:    $\text{block } r(s, d, b)$ 
4: else
5:   if  $C_{u,v,i} \neq \emptyset \forall i \geq b$  then
6:      $\text{establish } r(s, d, b)$  as  $P_n$ 
7:   else
8:      $(W(P_1), P_1) = \text{RSA-Flex}(G, r(s, d, b))$ 
9:      $(W(P_2), P_2) = \text{RSA-Flex}(G, r(s, d, b))$ 
10:    if  $W(P_1) = \infty$  or  $W(P_2) = \infty$  then
11:       $\text{block } r(s, d, b)$ 
12:    else
13:       $\text{establish } r(s, d, b)$  as  $P_n$ 
14:       $\text{establish } P_1$  and  $P_2$ 
15:       $\tilde{C}_{u,v,b} = P_1 \oplus P_2$ 
16:    end if
17:  end if
18: end if

```

para estabelecimento de caminhos ópticos chegam dinamicamente e para cada requisição tenta-se associar um p -cycle existente para proteger o caminho óptico requisitado. Caso não haja p -cycle que possa proteger o caminho óptico, então, cria-se um novo p -cycle para a requisição. Se nenhum caminho for encontrado para proteger o caminho solicitado, então ele não é estabelecido. O algoritmo FIPP-Flex garante um caminho de proteção para cada caminho óptico estabelecido e a proteção é garantida para falhas individuais. O algoritmo FIPP-Flex-twofailure diferentemente do algoritmo FIPP-Flex garante um caminho de proteção totalmente disjunto do caminho primário, e garante assim proteção para duas falhas simultâneas.

No algoritmo FIPP-Flex, a linha 1 tenta encontrar um caminho para estabelecer a requisição $r(s, d, b)$. Se não houver caminho disponível (linha 2), então o pedido é bloqueado (linha 3). Caso exista, procura-se um p -cycle para proteger o caminho solicitado (linha 5). Se existir um p -cycle, o caminho óptico é estabelecido. Caso contrário, tenta-se descobrir um p -cycle em potencial para proteger o caminho óptico solicitado (linhas 8 e 9). Se não existir nenhum p -cycle que possa ser criado para proteger o caminho óptico, a requisição é bloqueada (Linha 11); caso contrário, o caminho óptico (linha 13), bem como o p -cycle (linhas 14 e 15) são estabelecidos para satisfazer a requisição.

VII. AVALIAÇÃO DE DESEMPENHO

Nos experimentos de simulação, foi utilizado o simulador de eventos discretos *FlexGridSim* [12] desenvolvido em Java. A simulação de redes ópticas elásticas pode ser realizada levando-se em conta uma demanda de conexões estática, expressa através de uma matriz de tráfego, ou levando-se em conta uma demanda dinâmica de conexões, que escolhe aleatoriamente os pares origem destino de uma conexão, o tempo de início da conexão e o período de duração da conexão. O simulador *FlexGridSim* considera um modelo dinâmico de requisição de conexão. *FlexGridSim* possui um escalonador de eventos de conexão e de encerramento de conexão. No simulador foi acrescentado um escalonador de falha de enlace e de recuperação de falhas. Estes três tipos de eventos permite

a simulação de falhas em rede óptica com requisição dinâmica de conexões. O simulador admite como parâmetros de entrada: a topologia da rede, o tipo de mecanismo de proteção a ser simulado (algoritmo de proteção) e a taxa de falha de enlace.

No algoritmo proposto nesse artigo, a cada requisição de conexão, o algoritmo de roteamento e alocação de espectro (RSA) busca um caminho primário e outro secundário (backup), também chamado de proteção. Caso a rede consiga prover os dois canais, a conexão é estabelecida; caso contrário, a conexão não é estabelecida, ou seja ocorre uma situação de bloqueio de conexão. O algoritmo de RSA adotado é o RSA-Flex.

Para avaliar o desempenho dos algoritmos FIPP-Flex e FIPP-Flex-twofailure, foram empregados experimentos de simulação e os resultados comparados aos das redes sem qualquer esquema de proteção. O simulador *FlexGridSim* [12] foi utilizado nas simulações. Em cada simulação, 100.000 requisições foram geradas. Utilizou-se o método de replicação independente e adotou-se nível de confiança de 95 % para os intervalos de confiança. A topologia dfn-bwin-D-B-E-N-C-A-N-N (Figure 4) foi utilizada. Esta topologia contém tem 10 nós e 45 enlaces. Na rede elástica simulada, a análise do espectro foi dividido em 300 *slots* de 12,5 GHz cada.

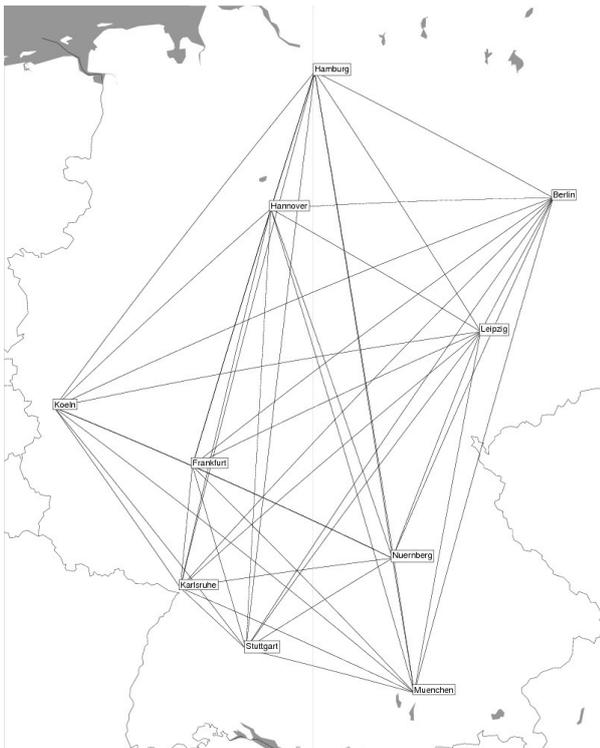


Figure 4: Topologia dfn-bwin-D-B-E-N-C-A-N-N

A Figura 5 mostra a probabilidade de sobrevivência da rede com proteção contra falha dupla. A curva rotulada como “FIPP-Flex” denota a rede protegida por *p-cycle* criado pelo algoritmo FIPP-Flex, a curva rotulados como “FIPP-Flex-twofailure” denota a rede protegida por *p-cycle* criado com

o algoritmo FIPP-Flex-twofailure, ou seja, a rede estará protegida contra duas falhas simultâneas. Embora o algoritmo FIPP-Flex não tenha sido projetado para proteção contra dupla falha, a probabilidade de sobrevivência foi plotada para o caso de dupla falha a fim de se avaliar a sua capacidade de prover proteção nestes casos. A probabilidade de sobrevivência contra duas falhas no algoritmo FIPP-Flex é 0,025. Embora este valor não seja aceitável para redes operacionais, ter uma garantia de probabilidade de sobrevivência de 0,025 sem ter que pagar o *overhead* associado para proteção de dupla falha é bastante vantajoso.

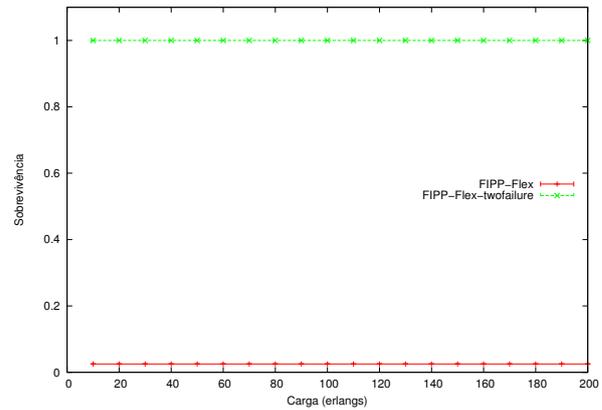


Figure 5: Sobrevivência

A Figura 6 apresenta o bloqueio de banda (*Bandwidth Blocking Ratio*) para redes sem proteção, com proteção contra uma falha e com proteção contra duas falhas. A curva rotulada com “No-FIPP-Flex” denota resultados para rede sem proteção. A BBR gerada para se ter proteção contra duas falhas está em torno de 0.5 devido a exigência de se ter três caminhos disjuncto o que faz com que alguns nós da rede sejam sobrecarregados mais rapidamente. A BBR gerada para se proteger uma única falha está em torno de 0.3. Há, portanto, um crescimento da BBR de 0,7 ao se garantir proteção contra dupla falha em relação à sem proteção. Observa-se que a partir da carga de 50 *erlangs*, o impacto no BBR para se proteger contra uma única falha é de aproximadamente 0,2, ou seja, bloqueia-se apenas 20 % a mais da banda requisitada do que em uma rede que não provê qualquer proteção de caminho.

A Figura 7 compara o número médio de saltos para o caminho primário. Observa-se que na rede com proteção contra falha dupla os caminhos são compostos por um maior número médio de saltos e que este decresce com o aumento da carga. Com o aumento da carga, diminui-se a disponibilidade de enlaces e aumenta-se o bloqueio da rede. Sob altas cargas, consegue-se estabelecer apenas caminhos menores. Vários caminhos que podem ser estabelecidos em redes sem proteção não podem ser estabelecidos em redes com proteção contra uma falha, conseqüentemente o tamanho médio dos caminhos em redes com proteção para uma falha são menores que os caminhos em redes com proteção.

Nas redes Flexgrid, o estabelecimento e rompimento de caminhos ópticos leva à fragmentação do espectro, que, é caracterizado pela existência de *slots* disponíveis que não podem

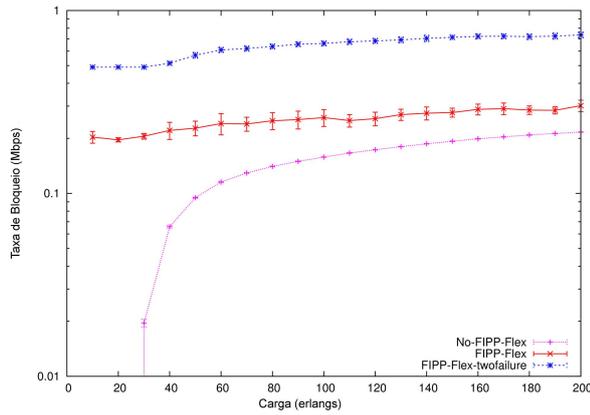


Figure 6: Bloqueio de banda em função da carga da rede

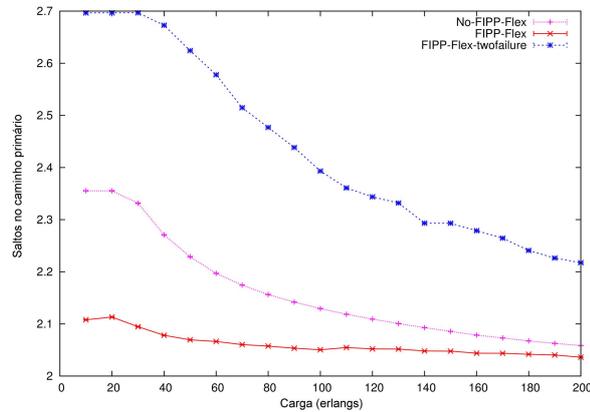


Figure 7: Tamanho médio dos saltos no caminho primário

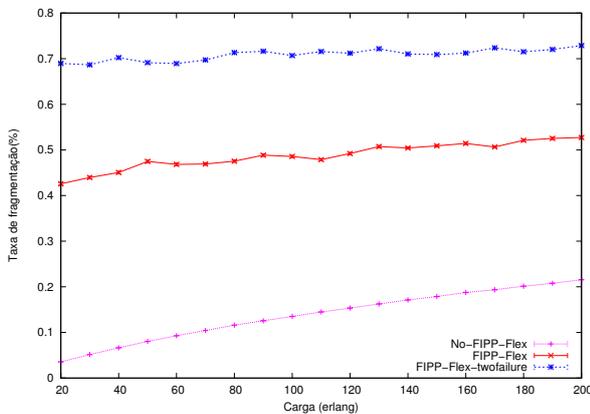


Figure 8: Relação de Fragmentação

ser aglutinados para aceitar requisições. Define-se razão de fragmentação como a razão entre a média do número de tipos de requisição (tamanho em slots) que não podem ser aceitas e o número total de tipos de requisição. A razão de fragmentação

indica a probabilidade de diferentes tipos de requisições serem rejeitadas como consequência da fragmentação. Há uma grande diferença entre os índices de fragmentação para redes sem proteção, com proteção contra uma falha e contra duas falhas. Quanto maior o grau de proteção, maior é a fragmentação da rede devido à alocação de maior número de caminhos de proteção de capacidade diversas.

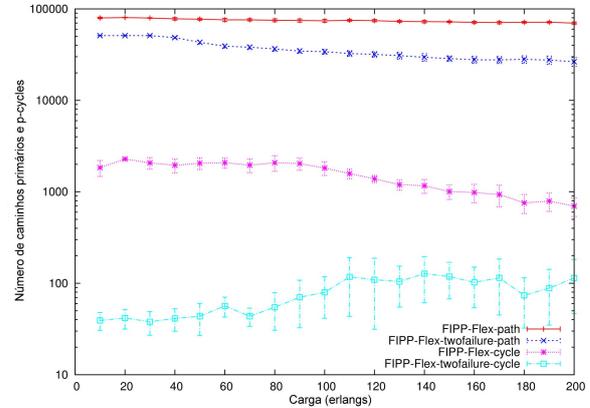


Figure 9: Número de Caminhos Primários e de p-Cycles em função da carga

A Figura 9 compara o número de *p-cycles* e caminhos primários estabelecidos. Observa-se que o número de caminhos primários estabelecidos ao se empregar o algoritmo FIPP-Flex difere em menos de uma ordem de grandeza do número de caminhos primários ao se utilizar o algoritmo FIPP-Flex-twofailure. No entanto, a diferença é de duas ordens de grandeza ao se comparar o número de *p-cycles* demandado. Dado que há mais bloqueio em redes que utilizam o algoritmo FIPP-Flex-twofailure, existe uma tendência para se estabelecer caminhos ópticos de proteção apenas para um número reduzido de *p-cycles*. Isto tende a aumentar o compartilhamento de *p-cycles*. Em redes que se utiliza o FIPP-Flex, um maior número de *p-cycles* com capacidade heterogênea é estabelecido e *p-cycles* tende a ser compartilhado por um número menor de caminhos primários.

VIII. CONCLUSÃO

Este artigo apresentou dois algoritmos para apoiar a criação de caminhos ópticos em redes *Flexgrid* protegidos por *p-cycles* FIPP para uma falha bem como para falhas duplas. Os algoritmos foram avaliados em diferentes cenários. O algoritmo FIPP-Flex fornece 100 % de proteção para falhas individuais e uma baixa sobrevivência para dupla falha. O algoritmo FIPP-Flex-twofailure provê 100 % de proteção contra duas falhas. No cenário com proteção contra única falha, é possível observar um impacto de até 20% no bloqueio de largura de banda. No cenário com proteção contra duas falhas a necessidade de se criar três caminhos disjuntos afeta significativamente o bloqueio de largura de banda causando sobrecarga e aumentando em mais 20 % o bloqueio em relação a redes protegidas contra uma falha única. Em ambos os cenários, o número de caminhos primários é maior que o número de *p-cycles*, já que os caminhos primários compartilham os *p-cycles*. O

número de caminhos primários para redes protegidas contra duas falhas é uma ordem de grandeza menor do que o número de caminhos primários protegidos contra uma única falha, além disso, o número de p-cycles é tipicamente uma ordem de grandeza maior. Como trabalho futuro diferentes esquemas de modulação e o impacto das condições de transmissão serão consideradas no algoritmo RSA.

REFERENCES

- [1] C. Xiaomin, A. Jukan, A. C. Drummond., and N. L. S. da Fonseca, "A multipath routing mechanism in optical networks with extremely high bandwidth requests," in *Proc of IEEE, Global Telecommunications Conference, 2009.*, 2009, pp. 1–6.
- [2] A. Pages, J. Perello, and S. Spadaro, "Lightpath fragmentation for efficient spectrum utilization in dynamic elastic optical networks," in *Optical Network Design and Modeling (ONDM), 2012 16th International Conference on*, April 2012, pp. 1–6.
- [3] T. Tanaka, A. Hirano, and M. Jinno, "Impact of transponder architecture on the scalability of optical nodes in elastic optical networks," *Communications Letters, IEEE*, vol. 17, no. 9, pp. 1846–1848, September 2013.
- [4] X. Shao, Y.-K. Yeo, Z. Xu, X. Cheng, and L. Zhou, "Shared-path protection in OFDM-based optical networks with elastic bandwidth allocation," in *Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2012 and the National Fiber Optic Engineers Conference, 2012*, pp. 1–3.
- [5] A. Patel, P. Ji, J. Jue, and T. Wang, "Survivable transparent flexible optical WDM (FWDM) networks," in *Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2011 and the National Fiber Optic Engineers Conference, 2011*, pp. 1–3.
- [6] M. Liu, M. Tornatore, and B. Mukherjee, "Survivable traffic grooming in elastic optical networks shared protection," *IEEE, Journal of Lightwave Technology*, vol. 31, no. 6, pp. 903–909, 2013.
- [7] R. Asthana, Y. Singh, and W. Grover, "p-cycles: An overview," *IEEE, Communications Surveys Tutorials*, vol. 12, no. 1, pp. 97 –111, quarter 2010.
- [8] M. Kiaei, C. Assi, and B. Jaumard, "A survey on the p-cycle protection method," *IEEE, Communications Surveys Tutorials*, vol. 11, no. 3, pp. 53 –70, quarter 2009.
- [9] Schupke, "Analysis of p-cycle capacity in WDM networks," *Photonic Network Communications*, pp. p. 41–51, 2006.
- [10] A. Kodian and W. Grover, "Failure-independent path-protecting pycles: efficient and simple fully preconnected optimal-path protection," *IEEE, J. Lightwave Technol.*, vol. 23, pp. 3241–3259, Oct. 2005.
- [11] Y. Wang, X. Cao, and Y. Pan, "A study of the routing and spectrum allocation in spectrum-sliced elastic optical path networks," in *Proc of IEEE, INFOCOM 2011*, 2011, pp. 1503–1511.
- [12] P. M. Moura and A. C. Drummond, "FlexGridSim: Flexible Grid Optical Network Simulator," <http://www.lrc.ic.unicamp.br/FlexGridSim/>.